**Devoir : Cybersécurité (20 points)**

**Questions :**

1. (2 pts) Définissez la cybersécurité et expliquez son importance.
2. (2 pts) Citez trois méthodes utilisées par les cybercriminels pour pirater un utilisateur.
3. (2 pts) Quels sont les trois principes fondamentaux de la protection des systèmes d'information ?
4. (2 pts) Qu'est-ce qu'un infostealer et quels types d'informations peut-il voler ?
5. (2 pts) Expliquez pourquoi l'activation de la double authentification est une mesure de sécurité efficace.
6. (2 pts) Quelles sont les conséquences légales encourues en cas de piratage informatique ?
7. (2 pts) Quels sont les risques encourus si une personne usurpe l'identité d'un autre en ligne ?
8. (2 pts) Pourquoi ne faut-il jamais désactiver son antivirus sur demande d'un logiciel ?
9. (2 pts) Donnez trois bonnes pratiques pour protéger ses mots de passe.
10. (2 pts) Que faire en cas de suspicion de cyberattaque sur ses comptes en ligne ?

**Corrigé :**

1. La cybersécurité consiste à protéger les données et les systèmes d'information contre les cybermenaces. Elle est essentielle pour garantir la confidentialité, l'intégrité et la disponibilité des données.
2. Phishing (hameçonnage), logiciels malveillants (malwares) et failles de sécurité exploitées par les hackers.
3. Confidentialité (seules les personnes autorisées accèdent aux données), intégrité (les données restent exactes et non altérées), disponibilité (les données sont accessibles quand nécessaire).
4. Un infostealer est un logiciel malveillant qui vole des informations telles que les mots de passe, les données bancaires ou encore les informations stockées dans un navigateur.
5. Elle empêche un pirate d'accéder à un compte même s'il possède le mot de passe, en demandant une validation supplémentaire (ex. : code envoyé par SMS).
6. Une personne reconnue coupable de piratage encourt jusqu'à 10 ans d'emprisonnement et des sanctions financières.
7. L'usurpation d'identité peut conduire à des poursuites judiciaires, car elle peut être utilisée pour commettre des fraudes ou des actes répréhensibles.
8. Certains logiciels demandent de désactiver l'antivirus pour installer un programme, mais cela permet souvent aux virus de s'introduire sans être détectés.
9. Utiliser des mots de passe forts et uniques, ne pas les stocker en clair, utiliser un gestionnaire de mots de passe.
10. Changer immédiatement ses mots de passe, activer la double authentification, et signaler l'incident sur des plateformes officielles comme 17cyber.gouv.fr.